Integer valued polynomials over function fields

by F.J. van der Linden*

Philips Research Laboratories WB3, P.O. Box 80000, 5600 JA Eindhoven, the Netherlands

Communicated by Prof. H.W. Lenstra at the meeting of January 25, 1988

ABSTRACT

Let A be an integrally closed subring of a function field K defined over a finite field. In this paper we investigate whether the subring of $K[X]$, consisting of those polynomials f with $f[A] \subset A$, has an A-basis $\{g_i : i \in \mathbb{Z}_{\geq 0}\}$, with $\deg(g_i) = i$.

INTRODUCTION

Let K be the function field of a complete, non-singular, irreducible curve $\mathscr{C}$ defined over the finite field $\mathbb{F}_q$ of q elements. For each extension field $\mathbb{F}$ of $\mathbb{F}_q$ we denote by $\mathscr{C}(\mathbb{F})$ the set of points of $\mathscr{C}$ defined over $\mathbb{F}$. Let G be the Galois group of the algebraic closure $\bar{\mathbb{F}}_q/\mathbb{F}_q$. The *divisor group Div* (K) of K is equal to the group of divisors of $\mathscr{C}(\bar{\mathbb{F}}_q)$ that are invariant under G, cf. [6] ch. II sect. 3. A *prime divisor* of K is a divisor that is equal to the sum of all elements of a conjugacy class of $\mathscr{C}(\bar{\mathbb{F}}_q)$ under G.

Let f be an element of K and let p be a prime divisor of K. We say that f has a zero or a pole of order n at p if it has such a zero or pole at some point P in the conjugacy class corresponding to p. This definition does not depend on the choice of P in this conjugacy class, cf. [6] ch. II sect. 3.

Let S be a non-empty set of prime divisors of K. Consider the ring

$$A_S = \{f \in K : f \text{ has no poles outside } S\}.$$

* Part of this research is supported by the Netherlands Organization for the Advancement of Pure Research (ZWO).

We call A_S a *Pólya-ring* if the ring $R_S = \{g \in K[X] : g[A_S] \subset A_S\}$ has, as an A_S-module, a basis $\{g_i : i \in \mathbb{Z}_{\geq 0}\}$, with $\deg(g_i) = i$. This definition is analogous to that of Zantema [8] in the number field case. Notice that, when $S \subset S'$ and A_S is a Pólya-ring, then $A_{S'}$ is a Pólya-ring as well. We can regard the polynomials g_i as playing the same role w.r.t. A_S as the polynomials $\binom{X}{i}$ do w.r.t. $\mathbb{Z}$, cf. [8].

In this paper we show how to determine whether a ring A_S is a Pólya-ring, using information about the Picard group of the curve, cf. lemma 4. This gives a partial answer to a question of M. van der Put [4] about Pólya-rings over function fields. Using this information the following results will be derived:

THEOREM 1. *Suppose that $K \simeq \mathbb{F}_q(X)$, then A_S is a Pólya-ring if and only if one of the following conditions is satisfied.*
(a) *A_S is a principal ideal domain.*
(b) *q is odd and A_S has class number equal to* 2.

PROOF. See theorem 7. □

THEOREM 2. *Suppose that q is odd and that $f \in \mathbb{F}_q[X]$ is a polynomial of odd degree with non-zero discriminant. Then $\mathbb{F}_q[X, Y]/(Y^2 - f)$ is a Pólya-ring if and only if all irreducible factors of f have the same degree.*

PROOF. See theorems 12, 25. □

In the second theorem K is the quotient field of $\mathbb{F}_q[X, Y]/(Y^2 - f)$, the function field of a curve which is hyperelliptic for $\deg(f) \geq 5$, elliptic for $\deg(f) = 3$ and rational for $\deg(f) = 1$. This field is a quadratic extension of $\mathbb{F}_q(X)$. In this case the set S is equal to the set consisting of the only prime lying over the infinite point of the projective line. Notice that for $\deg(f) = 1$ the second theorem is a consequence of the first one. If K is elliptic the theorem states that the ring is a Pólya-ring if and only if the polynomial f has no zero or f splits completely over $\mathbb{F}_q$. For elliptic fields we also give results for other sets S than the one given in theorem 2, cf. theorems 12 and 23. The case with even q is investigated as well. In section 4 we treat completely the case that K is elliptic and S consists of all primes of a given degree, cf. theorem 23.

In the final section we will give some examples of rings that are Pólya-rings and some that are not, thus illustrating the theory.

1. NOTATIONAL ISSUES

Let $a = \sum_{P \in \mathscr{C}(\mathbb{F}_q)} n(P)P \in Div(K)$ be a divisor. The *degree* of a is defined by $\deg(a) = \sum_{P \in \mathscr{C}/\mathbb{F}_q} n(P) \in \mathbb{Z}$. The subgroup $Div(K)$ of divisors of degree 0 will be denoted by $Div_0(K)$ and the subgroup of *principal divisors*, i.e., divisors of the form $(f) = \sum\{\text{zeroes of } f\} - \sum\{\text{poles of } f\}$, for some $f \in K^*$, will be denoted by $P(K)$. A *positive divisor* is a divisor in which all coefficients are non

negative, and there is at least one positive coefficient. A *prime divisor* of K is a divisor of the form $\sum\{P: P \in C\}$, where C is an orbit of $\mathscr{C}(\bar{\mathbb{F}}_q)$ under G. These are exactly the positive divisors that are not sums of other positive divisors. The divisor group $Div(K)$ is freely generated by the prime divisors of K, cf. [6] ch. II sect. 3.

The *class group* (or *Picard group*) of K is the quotient group $\mathscr{Cl}(K) = Div(K)/P(K)$. The class of a divisor a will be denoted by $[a]$. Because principal divisors have degree equal to 0, cf. [1] sect. 11 cor. 1, we may define the degree $\deg([a])$ of the divisor class $[a]$ to be equal to $\deg(a)$. The subgroup of $\mathscr{Cl}(K)$ consisting of the divisor classes of degree 0 will be denoted by $\mathscr{Cl}_0(K)$. For any subgroup B of $\mathscr{Cl}(K)$ we write $B_0 = B \cap \mathscr{Cl}_0(K)$. If B is written with some arguments we usually write the index 0 before the brackets. Notice that $\mathscr{Cl}_0(K)$ is equal to the set of points of the Jacobian of $\mathscr{C}$, defined over $\mathbb{F}_q$, cf. [6] ch. II sect. 3. For $d \in \mathbb{Z}_{>0}$ we denote by $\mathscr{Cl}_d(K)$ the subgroup of $\mathscr{Cl}(K)$, consisting of all divisors of degree divisible by d.

Because the degree map: $\mathscr{Cl}(K) \to \mathbb{Z}$ is surjective, cf. [1] sect. 39, we have an exact sequence

$$0 \to \mathscr{Cl}_0(K) \to \mathscr{Cl}(K) \xrightarrow{\deg} \mathbb{Z} \to 0$$

For the sequel we choose an element $[a] \in \mathscr{Cl}(K)$ of degree 1 fixed. This element gives rise to an isomorphism

$$\phi_a: \mathscr{Cl}(K) \xrightarrow{\sim} \mathscr{Cl}_0(K) \oplus \mathbb{Z}$$

$$[b] \mapsto ([b - \deg(b) \cdot a], \deg(b))$$

Notice that for any subgroup $B \subset \mathscr{Cl}(K)$ we have $\phi_a[B] \cap (\mathscr{Cl}_0(K) \oplus \{0\}) = B_0 \oplus \{0\}$.

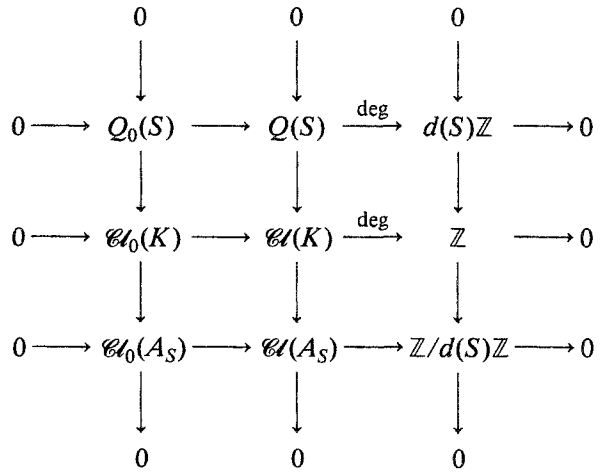
The prime divisors of K, not in S, are in $1-1$ correspondence with the non-zero prime ideals of A_S. This correspondence is given by

$$p \leftrightarrow \{f \in A_S : f \text{ has a zero at } p\}.$$

If we denote the subgroup of $Div(K)$ generated by the prime divisors in S by $\Gamma(S)$ and its image in $\mathscr{Cl}(K)$ by $Q(S)$ we find that the ideal group of A_S is isomorphic to $Div(K)/\Gamma(S)$ and the ideal class group $\mathscr{Cl}(A_S)$ is isomorphic to $\mathscr{Cl}(K)/Q(S)$. Notice that the sum of divisors corresponds to products of ideals.

For $k \in \mathbb{Z}_{>0}$ we denote the number of elements of $\mathscr{C}(\mathbb{F}_{q^k})$ by $n(k)$. The greatest common divisor of the degrees of the primes in S will be denoted by $d(S)$. We write $\mathscr{Cl}_0(A_S) = \mathscr{Cl}_0(K)/Q_0(S)$, the subgroup of $\mathscr{Cl}(A_S)$ generated by divisors of degree 0.

The following diagram with exact rows and columns shows the connections between the different groups.



For $k \in \mathbb{Z}_{>0}$ we define $\mathscr{P}(k)$ to be the set of prime ideals of A_S of norm q^k. Notice that the prime ideals in $\mathscr{P}(k)$ are in $1-1$ correspondence with the prime divisors of K, not in S, of degree k.

2. PROPERTIES OF CLASS GROUPS OF PÓLYA-RINGS

Analogously to the number field case we have the following result.

PROPOSITION 3. *The ring A_S is a Pólya-ring if and only if for each $k \in \mathbb{Z}_{>0}$ the A_S-ideal $\prod_{p \in \mathscr{P}(k)} p$ is principal.*

PROOF. Analogous to the proof of Zantema [8] thm. 2.3. □

For $k \in \mathbb{Z}_{>0}$ we write

$$B(k, a) = \sum_{P \in \mathscr{C}(\mathbb{F}_{q^k})} [P - a] \in \mathscr{C}\ell(K).$$

Notice that $B(k, a)$ is in $\mathscr{C}\ell_0(K)$. A different choice of $[a]$ may change $B(k, a)$ by an element of $n(k) \cdot \mathscr{C}\ell_0(K)$.

LEMMA 4. *The ring A_S is a Pólya-ring if and only if for all $k \in \mathbb{Z}_{>0}$ we have $(B(k, a), n(k)) \in \phi_a[Q(S)]$.*

PROOF. We have

A_S is a Pólya-ring $\Leftrightarrow$

$\Leftrightarrow \sum_{\substack{\deg(q)=k \\ q \notin S}} [q] \in Q(S)$ for all $k \in \mathbb{Z}_{>0}$, by proposition 3

$\Leftrightarrow \sum_{\deg(q)=k} [q] \in Q(S)$ for all $k \in \mathbb{Z}_{>0}$, because the primes in S generate $Q(S)$

$$\Leftrightarrow \sum_{\deg(q)\mid k} [q] \in Q(S) \qquad \text{for all } k \in \mathbb{Z}_{>0}, \qquad \text{by Moebius inversion}$$

$$\Leftrightarrow \sum_{P \in \mathscr{C}(\mathbb{F}_{q^k})} [P] \in Q(S) \qquad \text{for all } k \in \mathbb{Z}_{>0}, \qquad \text{because } \mathscr{C}(\mathbb{F}_{q^k}) \text{ consists exactly of all points that compose into the primes of degree dividing } k$$

$$\Leftrightarrow n(k) \cdot [a] + B(k, a) \in Q(S) \qquad \text{for all } k \in \mathbb{Z}_{>0}.$$

Because $\phi_a(n(k) \cdot [a] + B(k, a)) = (B(k, a), n(k))$ this proves the lemma. □

By inspecting the second component of $\mathscr{U}(K) \times \mathbb{Z}$ we derive the following corollaries.

COROLLARY 5. *If A_S is a Pólya-ring then $d(S)$ divides* $\gcd(n(k) : k \in \mathbb{Z}_{>0})$. □

COROLLARY 6. *If $\mathscr{U}_0(A_S) = 0$ then A_S is a Pólya-ring if and only if* $d(S) \mid \gcd(n(k) : k \in \mathbb{Z}_{>0})$. □

For the case that the genus of K is equal to 0 we find that corollary 6 boils down to the following:

THEOREM 7. *Suppose that K is a function field of genus 0 defined over $\mathbb{F}_q$ and that S is a non-empty set of prime divisors of K. Then the ring A_S is a Pólya-ring if and only if one of the following conditions is satisfied.*
(a) $d(S) = 1$;
(b) $d(S) = 2$ *and q is odd.*

PROOF. We use the fact that $\mathscr{U}_0(K) = 0$, cf. [1] sect. 18, thus $\mathscr{U}_0(A_S) = 0$ for all choices of S. Hence A_S is a Pólya-ring if and only if $d(S) \mid \gcd(n(k) : k \in \mathbb{Z}_{>0})$. By [2] ch. 8 sect. 1 cor. 1 we have $n(k) = q^k + 1$, hence

$$\gcd(n(k) : k \in \mathbb{Z}_{>0}) = 1 \quad \text{if } q \text{ is even;}$$

$$\gcd(n(k) : k \in \mathbb{Z}_{>0}) = 2 \quad \text{if } q \text{ is odd.}$$ □

Because in the case that $g = 0$ the class number of A_S is equal to $d(S)$ we derive theorem 1.

3. FIELDS OF GENUS 1

In this section and the next we suppose that the genus of K is equal to 1. It can be shown that $\mathscr{C}(\mathbb{F}_q)$ has at least one point, cf. [3] ch. 8 sect. 2 thm. 2, [6] ch. V sect. 1 thm. 1.1. In this section we take for the divisor a of degree 1 the divisor of a point $P_0 \in \mathscr{C}(\mathbb{F}_q)$.

For each extension field $\mathbb{F}$ of $\mathbb{F}_q$ the curve $\mathscr{C}(\mathbb{F})$ forms in a natural way a group with P_0 as zero element. In the sequel we only consider the case that $\mathbb{F}$ is an algebraic extension of $\mathbb{F}_q$, but many of the following results can be generalized to other extensions as well. The group structure is inherited from the class group $\mathscr{C}\ell_0(K\otimes\mathbb{F})$, of the curve, since by the Riemann-Roch theorem the map $\mathscr{C}(\mathbb{F})\to\mathscr{C}\ell_0(K\otimes\mathbb{F})$, given by $P\mapsto[P-P_0]$ is in fact a bijection, cf. [1] sect. 15 p. 40, [6] ch. III sect. 3 prop. 3.4. The group structure is such that $\mathscr{C}(\mathbb{F}_q)$ is a subgroup of $\mathscr{C}(\mathbb{F})$, for each extension field $\mathbb{F}$ of $\mathbb{F}_q$. In particular $\mathscr{C}(\mathbb{F}_q)$ is a subgroup of $\mathscr{C}(\mathbb{F}_{q^k})$, which shows that $\gcd(n(k):k\in\mathbb{Z}_{>0})=n(1)$. From now on we assume that $d(S)$ divides $n(1)$, which by corollary 5 is a necessary condition for A_S to be a Pólya-ring. For each $k\in\mathbb{Z}_{>0}$, let $T(k)$ be the 2-power-torsion subgroup of $\mathscr{C}\ell(K\otimes\mathbb{F}_{q^k})$ and let $T(\infty)$ be the 2-power-torsion subgroup of $\mathscr{C}\ell(K\otimes\bar{\mathbb{F}}_q)$. Notice that $T(\infty)$ is the union of the groups $T(k)$, for $k\in\mathbb{Z}_{>0}$. If $G_k\subset G$ is the Galois group of $\bar{\mathbb{F}}_q/\mathbb{F}_{q^k}$, then $T(k)$ is the subgroup of $T(\infty)$ consisting of all elements fixed under G_k.

LEMMA 8. *For each $k\in\mathbb{Z}_{>0}$, the class $B(k,P_0)$ is the unique element of order 2 in $T(k)$ if $T(k)$ is cyclic of order >1 and $B(k,P_0)=0$ otherwise.*

REMARK 9. *Notice that in the case that $g=1$ the class $B(k,P_0)$ does not depend on the choice of P_0.*

PROOF. The sum of all elements of a finite abelian group is equal to the unique element of order 2 if there is such a unique element and it is equal to 0 otherwise. □

The group $T(\infty)$ is isomorphic to $(\mathbb{Q}_2/\mathbb{Z}_2)^2$ if q is odd and $T(\infty)$ is isomorphic to $\mathbb{Q}_2/\mathbb{Z}_2$ (the ordinary case) or 0 (the supersingular case) if q is even, cf. [7] thm. 1, [6] ch. III sect. 6 cor. 6.4.

LEMMA 10. *Suppose that $T(1)$ is of order >1 and suppose that $k\in\mathbb{Z}_{>0}$ is such that $T(k)\neq T(1)$, then k is even.*

PROOF. Let $\mathscr{A}$ be the image of $\mathrm{Gal}(\mathbb{F}_{q^k}/\mathbb{F}_q)$ in $\mathrm{Aut}(T(k))$. Then $T(1)$ is the set of fixed points of $\mathscr{A}$ in $T(k)$. Notice that $\mathscr{A}\neq\{id\}$ because $T(k)\neq T(1)$. Let σ be an element of $\mathscr{A}$ of odd order n. The stabilizer $T(k)^{\langle\sigma\rangle}$ is as an $\mathscr{A}$-module a direct summand of $T(k)$, since $1/n\sum_{i=0}^{n-1}\sigma^i$ maps $T(k)$ onto $T(k)^{\langle\sigma\rangle}$ and it is the identity on the latter group. The rank of $T(k)$ is at most 2 and $T(k)^{\langle\sigma\rangle}\neq 1$ (it contains $T(1)$), thus $T(k)=T(k)^{\langle\sigma\rangle}\oplus U$, for some $\mathscr{A}$-module $U\subset T(k)$, which is cyclic as group. Each non-trivial automorphism of a cyclic group of 2-power order has even order, thus σ acts trivially on U, i.e., $U=1$ and $\sigma=id$. This shows that all nontrivial elements of $\mathscr{A}$ have even order. In particular $\#\mathrm{Gal}(\mathbb{F}_{q^k}/\mathbb{F}_q)=k$ is even. □

LEMMA 11

(a) *If $T(1)$ does not have a unique element of order 2 then no $T(k)$ has such an element.*

(b) *If $T(1)$ has a unique element of order 2 and q is odd then $T(k)$ has a unique element of order 2 if and only if k is odd. The quotient $n(k)/n(1)$ has the same parity as k has.*

(c) *If $T(1)$ has a unique element of order 2 and q is even then each $T(k)$ has a unique element of order 2 for all $k \in \mathbb{Z}_{>0}$. The quotient $n(k)/n(1)$ has the same parity as k has.*

PROOF

(a) If $T(k)$ has a unique element of order 2 then this element is invariant under G, hence this element is in $T(1)$.

(b) Let $[c]$ be the unique element of order 2 in $T(1)$ and let $[d_1]$ and $[d_2]$ be the other elements of order 2 of $T(\infty)$. The group G leaves the set $\{[d_1], [d_2]\}$ invariant, hence $[d_1]$ and $[d_2]$ are defined over $\mathbb{F}_{q^2}$, and thus they are in $T(2)$. This shows that $T(2k)$ is *not* cyclic for any $k \in \mathbb{Z}_{>0}$ and $n(2k)/n(1)$ is even. Together with lemma 10 this shows that $n(k)/n(1)$ has the same parity as k.

(c) There is at most one element of order 2 in $T(k)$, hence there is exactly one element of order 2 in $T(k)$ for all $k \in \mathbb{Z}_{>0}$. Let $[d_1]$ and $[d_2]$ be the two elements of order 4 of $T(\infty)$. As in (b) these elements are in $T(2)$ and the parity of $n(k)/n(1)$ is equal to that of k. □

THEOREM 12. *Let K be a function field of genus 1, defined over the finite field $\mathbb{F}_q$. The number of elements of $\mathscr{C}(\mathbb{F}_q)$ is denoted by $n(1)$ and the 2-power torsion subgroup of $\mathscr{C}(\mathbb{F}_q)$ is denoted by $T(1)$, as at the beginning of this section. The greatest common divisor of the primes in S is denoted by d. Then the ring A_S is a Pólya-ring if and only if $d \mid n(1)$ and we are in one of the following cases:*

(a) *$T(1)$ does not have a unique element of order 2 and $(0, n(1)) \in \phi_{P_0}[Q(S)]$;*

(b) *$T(1)$ has a unique element $[c]$ of order 2, q is odd and $([c], n(1)) \in \phi_{P_0}[Q(S)]$;*

(c) *$T(1)$ has a unique element $[c]$ of order 2, q is even and $(0, n(1)), ([c], 0) \in \in \phi_{P_0}[Q(S)]$.*

PROOF

(a) If $T(1)$ does not have a unique element of order 2 then by lemma 11(a) no $T(k)$ has such an element. Thus, using lemma 8, we find that $B(k, P_0) = 0$ for all $k \in \mathbb{Z}_{>0}$. By lemma 4 this shows that A_S is a Pólya-ring if and only if $(0, n(k)) \in \phi_{P_0}[Q(S)]$ for all $k \in \mathbb{Z}_{>0}$. Because $n(1) \mid n(k)$ for all $k \in \mathbb{Z}_{>0}$ this is equivalent to $(0, n(1)) \in \phi_{P_0}[Q(S)]$.

(b) If $T(1)$ has a unique element $[c]$ of order 2 and q is odd then from lemma 8 and lemma 11(b) we derive that $B(k, P_0) = [c]$ if k is odd and $B(k, P_0) = 0$ if k is even. Hence the condition of lemma 4 is equivalent to $([c], n(k)) \in \phi_{P_0}[Q(S)]$ for odd k and $(0, n(k)) \in \phi_{P_0}[Q(S)]$ for even k. Because $n(1) \mid n(k)$ for all $k \in \mathbb{Z}_{>0}$, the order of $[c]$ equals 2 and $(n(k)/n(1))$ has the same parity as k this is equivalent to $([c], n(1)) \in \phi_{P_0}[Q(S)]$.

(c) If $T(1)$ has a unique element $[c]$ of order 2 and q is even then from lemma 8 and lemma 11(c) we derive that $B(k, P_0) = [c]$ for all $k \in \mathbb{Z}_{>0}$. Hence A_S is a Pólya-ring if and only if $([c], n(k)) \in \phi_{P_0}[Q(S)]$ for all $k \in \mathbb{Z}_{>0}$. Because $n(1) \mid n(k)$ and $n(k)/n(1)$ attains both odd and even values we find that the condition of lemma 4 is equivalent to $(0, n(1)), ([c], 0) \in \in \phi_{P_0}[Q(S)]$. □

Notice that in the case that q is even we always have to apply 12(a) in the supersingular case and we have to apply 12(c) in the ordinary case.

COROLLARY 13. *Suppose that* $d(S) = 1$.
(a) *If* $T(1)$ *does not have a unique element of order* 2 *then* A_S *is a Pólya-ring.*
(b) *If* $T(1)$ *has a unique element* $[c]$ *of order* 2 *then* A_S *is a Pólya-ring if and only if* $[c] \in Q_0(S)$.

PROOF. Let $[b]$ be an element of $Q(S)$ of degree 1. Then $\phi_{P_0}(b) = (x, 1)$ for some $x \in \mathscr{C}\ell_0(K)$, so $n(1) \cdot (x, 1) = (0, n(1)) \in \phi_{P_0}[Q(S)]$. The result follows from the fact that $\phi_{P_0}[Q(S)] \cap (\mathscr{C}\ell_0(K) \oplus \{0\}) = Q_0(S) \oplus \{0\}$. □

4. SETS CONTAINING ALL PRIMES OF A GIVEN DEGREE

In this section we still assume that K is an elliptic function field. Now we consider a special case. Let $S = S(q, k)$ be the set of all primes of a fixed degree k, for some $k \in \mathbb{Z}_{>0}$. We only consider the case that $S(q, k)$ is non-empty. From corollary 5 we see that $k \mid n(1)$ if $A_{S(q,k)}$ is a Pólya-ring. Below we see that, but for one exception, the converse holds as well. In order to derive this result we investigate a trace function.

The field $K \otimes \mathbb{F}_{q^k}$ is the function field of $\mathscr{C}$ over $\mathbb{F}_{q^k}$. We have trace maps for $\ell \mid k$:

$$\mathrm{Tr}_{k,\ell} \colon \mathscr{C}\ell(K \otimes \mathbb{F}_{q^k}) \to \mathscr{C}\ell(K \otimes \mathbb{F}_{q^\ell})$$

$$[b] \mapsto \Big[\sum_{\sigma \in \mathrm{Gal}(\mathbb{F}_{q^k}/\mathbb{F}_{q^\ell})} \sigma b \Big]$$

Notice that these are well defined homomorphisms and that $\mathrm{Tr}_{k,\ell} \circ \mathrm{Tr}_{m,k} = \mathrm{Tr}_{m,\ell}$. The image of $\mathrm{Tr}_{k,\ell}$ is contained in the subgroup $\mathscr{C}\ell_{k/\ell}(K \otimes \mathbb{F}_{q^\ell})$ of $\mathscr{C}\ell(K \otimes \mathbb{F}_{q^\ell})$, consisting of all divisor classes of a degree divisible by k/ℓ. In fact we have a stronger result.

PROPOSITION 14. *The image of* $\mathrm{Tr}_{k,\ell}$ *is equal to* $\mathscr{C}\ell_{k/\ell}(K \otimes \mathbb{F}_{q^\ell})$. *Each class in* $\mathscr{C}\ell_{k/\ell}(K \otimes \mathbb{F}_{q^\ell})$ *is the image of exactly* $n(k)/n(\ell)$ *classes of* $\mathscr{C}\ell(K \otimes \mathbb{F}_{q^k})$.

PROOF. We can extend $\mathrm{Tr}_{k,\ell}$ to an endomorphism of $\mathscr{C}\ell(K \otimes \bar{\mathbb{F}}_q)$, as a sum of powers of the frobenius map. When restricted to $\mathscr{C}\ell_0(K \otimes \bar{\mathbb{F}}_q)$ it is a nontrivial isogeny, cf. [6] ch. III sect. 4 example 4.6, thus it is a surjective homomor-

phism. The elements of $\mathscr{C}\ell_0(K\otimes\mathbb{F}_{q^\ell})$ are exactly the images of the elements of $\mathscr{C}\ell_0(K\otimes\mathbb{F}_{q^k})$. This shows that $\mathrm{Tr}_{k,\ell}$ maps $\mathscr{C}\ell(K\otimes\mathbb{F}_{q^k})$ surjectively onto $\mathscr{C}\ell_{k/\ell}(K\otimes\mathbb{F}_{q^\ell})$. The kernel of $\mathrm{Tr}_{k,\ell}$ contains exactly $n(k)/n(\ell)$ elements, which proves the second assertion. □

A similar theorem holds in the case that K has an arbitrary genus. We define

$$\mathscr{C}'_q(\mathbb{F}_{q^k}) = \mathscr{C}(\mathbb{F}_{q^k}) - \bigcup_{\substack{\ell\mid k\\ \ell\neq k}} \mathscr{C}(\mathbb{F}_{q^\ell}),$$

the set of points of $\mathscr{C}(\mathbb{F}_{q^k})$ that are not defined over any intermediate field of $\mathbb{F}_{q^k}/\mathbb{F}_q$. Notice that this is the subset of $\mathscr{C}(\mathbb{F}_{q^k})$ of points that are not left fixed by any non-trivial element of $\mathrm{Gal}(\mathbb{F}_{q^k}/\mathbb{F}_q)$. We denote by $\mathbf{Q}(q, q^k)$ the subgroup of $\mathscr{C}\ell(K\otimes\mathbb{F}_{q^k})$ generated by the classes $[P]$ for $P\in\mathscr{C}'_q(\mathbb{F}_{q^k})$. We have $Q(S(q,k)) = \mathrm{Tr}_{k,1}[\mathbf{Q}(q,q^k)]$.

LEMMA 15. *All elements of $\mathscr{C}\ell_0(K)$ that are differences of two elements that are not in $p\mathscr{C}\ell_0(K)$ for any prime $p\mid k$ are contained in $Q(S(q,k))$.*

PROOF. Choose $P_0\in\mathscr{C}(\mathbb{F}_q)$. Under $\phi_{P_0}\circ\mathrm{Tr}_{k,1}$ the classes of points of $\mathscr{C}(\mathbb{F}_{q^k})$ are mapped onto $\mathscr{C}\ell_0(K)\times\{k\}$. For $\ell\mid k$ the elements of $\mathscr{C}(\mathbb{F}_{q^\ell})$ are mapped onto $k/\ell\,\mathscr{C}\ell_0(K)\times\{k\}$. Thus all classes in $(\mathscr{C}\ell_0(K) - \bigcup_{p\mid k} p\mathscr{C}\ell_0(K))\times\{k\}$ are contained in $\phi_{P_0}[Q(S(q,k))]$. By taking differences of these classes we derive the assertion. □

REMARK 16. *Notice that, when $k\mid n(1)$, we always have $S(q,k)\neq\emptyset$.*

PROOF. $(\mathscr{C}\ell_0(K) - \bigcup_{p\mid k} p\mathscr{C}\ell_0(K))\times\{k\}\subset\phi_{P_0}[\mathscr{C}'_q(\mathbb{F}_{q^k})]$ and the former set is nonempty. □

In order to investigate $Q(S(q,k))$ we need a group theoretic result.

LEMMA 17. *Let G be a finite abelian group and let $\mathscr{P}$ be a set of prime numbers, all dividing the order of G. Let H be the subgroup of G generated by $\{g_1-g_2 : g_i\in G - \bigcup_{p\in\mathscr{P}} pG\}$, i.e., the differences of elements of G that are not in any pG, for $p\in\mathscr{P}$. We have the following equalities:*
(a) *$H=G$ if $2\notin\mathscr{P}$;*
(b) *$H=G$ if $2\in\mathscr{P}$ and the 2-torsion subgroup of G is noncyclic;*
(c) *$H=2G$ if $2\in\mathscr{P}$ and the 2-torsion subgroup of G is cyclic.*

PROOF. Let $\mathscr{Q}$ be the set of all primes dividing $\#G$. We have $\mathscr{P}\subset\mathscr{Q}$. We may write $G\simeq\bigoplus_{p\in\mathscr{Q}} G_p$, where G_p is the p-torsion subgroup of G. For each $g\in G$ we may write $g=\sum_{p\in\mathscr{Q}} g_p$, with $g_p\in G_p$.

For the cases (a) and (b) we may suppose that either $2\notin\mathscr{P}$ or $2\in\mathscr{P}$ and G_2 is noncyclic. Thus we have $\#(G_p/pG_p)\geq 3$ for all $p\in\mathscr{P}$. Take $g=\sum_{p\in\mathscr{Q}} g_p\in G$.

There exists $h=\sum_{p\in\mathscr{P}} h_p \in G$ such that $h_p \notin p\,G_p$ and $h_p \neq -g_p$ for all $p\in\mathscr{P}$. Then both h and $h+g$ are not in pG for all $p\in\mathscr{P}$, thus $g=(h+g)-h\in H$.

For the case (c) we suppose that $2\in\mathscr{P}$ and that G_2 is cyclic. For each pair $\sum_{p\in\mathscr{P}} g_p$, $\sum_{p\in\mathscr{P}} g'_p \in G-\bigcup_{p\in\mathscr{P}} pG$ we have $(g_2-g'_2)\in 2G_2$, thus $H\subset 2G$. Suppose that $g=\sum_{p\in\mathscr{P}} g_p \in 2G$, then $g_2\in 2G_2$. There exists $h=\sum_{p\in\mathscr{P}} h_p\in G$, such that $h_p\notin p\,G_p$ and $h_p\neq -g_p$ for all $p\in\mathscr{P}$. Again we deduce that $g=(h+g)-h\in H$. □

COROLLARY 18. *Suppose that $k\,|\,n(1)$. If k is odd, or k is even and $T(1)$ is noncyclic, then $Q(S(q,k))=\mathscr{C}\ell_k(K)$, otherwise $[\mathscr{C}\ell_k(K):Q(S(q,k))]\leq 2$.* □

Notice that from corollary 6 we derive that in the cases that $\mathscr{C}\ell_k(K)=Q(S(q,k))$ the ring $A_{S(q,k)}$ is a Pólya-ring. Next we investigate the cases in which k is even and $T(1)$ is cyclic.

LEMMA 19. *Suppose that $k\,|\,n(1)$, that $k=2\ell$, that ℓ is even and that $Q(S(q^2,\ell))=\mathscr{C}\ell_\ell(K\otimes\mathbb{F}_{q^2})$, then $Q(S(q,k))=\mathscr{C}\ell_k(K)$.*

PROOF. Since ℓ is even we have $\mathscr{C}'_{q^2}(\mathbb{F}_{q^k})=\mathscr{C}'_q(\mathbb{F}_{q^k})$. Hence we have the following equalities:

$$Q(S(q,k))=\mathrm{Tr}_{k,1}[\mathbf{Q}(q,q^k)]=\mathrm{Tr}_{k,1}[\mathbf{Q}(q^2,q^k)]=$$
$$=\mathrm{Tr}_{2,1}[\mathrm{Tr}_{k,2}[\mathbf{Q}(q^2,q^{2\ell})]]=\mathrm{Tr}_{2,1}[Q(S(q^2,\ell))]=$$
$$=\mathrm{Tr}_{2,1}[\mathscr{C}\ell_\ell(K\otimes\mathbb{F}_{q^2})]=\mathscr{C}\ell_k(K).$$ □

COROLLARY 20. *If $4\,|\,k$, $k\,|\,n(1)$ and q is odd, then $Q(S(q,k))=\mathscr{C}\ell_k(K)$.*

PROOF. Notice that in this case $T(2)$ is not cyclic. □

LEMMA 21. *Suppose that $k\,|\,n(1)$, that $k=2\ell$, that ℓ is odd, that $T(1)$ is cyclic and that $n(k)\neq 2n(\ell)$, then $Q(S(q,k))=\mathscr{C}\ell_k(K)$.*

PROOF. The map $\mathrm{Tr}_{k,\ell}$ has degree $n(k)/n(\ell)\neq 2$. When restricted to $\mathscr{C}\ell(K\otimes\mathbb{F}_{q^\ell})$ it has a kernel of size 2 and the image is $2\mathscr{C}\ell(K\otimes\mathbb{F}_{q^\ell})$. Thus, the classes of points in $\mathscr{C}'_{q^\ell}(\mathbb{F}_{q^k})$ map surjectively onto the elements of $\mathscr{C}\ell(K\otimes\mathbb{F}_{q^\ell})$ of degree 2.

Let P_0 be an element of $\mathscr{C}(\mathbb{F}_q)$. Choose $P\in\mathscr{C}'_q(\mathbb{F}_{q^\ell})$. There exists $P'\in\mathscr{C}'_{q^\ell}(\mathbb{F}_{q^k})$ such that $\mathrm{Tr}_{k,\ell}(P')=P+P_0$. Since $\sigma(P+P_0)\neq(P+P_0)$ for all $\sigma\in\mathrm{Gal}(\mathbb{F}_{q^\ell}/\mathbb{F}_q)$ we find that $\tau P'\neq P'$ for all $\tau\in\mathrm{Gal}(\mathbb{F}_{q^k}/\mathbb{F}_q)$. Thus $P'\in\mathscr{C}'_q(\mathbb{F}_{q^k})$. By taking differences we find that $\mathbf{Q}_0(q,q^\ell)\subset\mathrm{Tr}_{k,\ell}[\mathbf{Q}_0(q,q^k)]$. Because $\mathrm{Tr}_{\ell,1}[\mathbf{Q}_0(q,q^\ell)]=\mathscr{C}\ell_0(K)$, by corollary 18, we find that $\mathrm{Tr}_{k,1}[q,q^k)]=\mathscr{C}\ell_0(K)$ and thus $\mathrm{Tr}_{k,1}[\mathbf{Q}(q,q^k)]=\mathscr{C}\ell_k(K)$. □

There are not many cases where $k=2\ell$ and $n(k)=2n(\ell)$:

LEMMA 22. *Suppose that $k=2\ell$ and that $n(k)=2n(\ell)$, then $n(\ell)=2q^\ell$ and $q^\ell\leq 5$.*

PROOF. There exists $\pi \in \mathbb{C}$ with $|\pi| = \sqrt{q^\ell}$, such that

$$n(\ell) = q^\ell + 1 - \pi - \bar{\pi} \text{ and}$$

$$n(k) = q^k + 1 - \pi^2 - \bar{\pi}^2,$$

cf. [6] ch. V sect. 2; [7] sect. 5 thm. 2. This shows that $n(k) = n(\ell)(2q^\ell + 2 - n(\ell))$. Since $n(k) = 2n(\ell)$ we find that $n(\ell) = 2q^\ell$. Because $|\pi| = \sqrt{q^\ell}$ we have

$$q^\ell - 1 = n(\ell) - q^\ell - 1 \leq 2\sqrt{q^\ell}.$$

This is only possible when $q^\ell \leq 5$. □

THEOREM 23. *Let K be an elliptic field, defined over $\mathbb{F}_q$. Suppose that $k \in \mathbb{Z}_{>0}$ is such that that $k \mid n(1)$. The set of all primes of degree k in K is denoted by $S(q, k)$. Then the ring $A_{S(q,k)}$ is a Pólya-ring except in the case that $q = 2$ and $n(1) = k = 4$.*

PROOF. Notice that $S(q, k)$ is nonempty, cf. remark 16. If $Q(S(q, k)) = \mathscr{C}\ell_k(K)$ then $A_{S(q,k)}$ is a Pólya-ring, since by theorem 12 we only need the existence of certain elements of $\mathscr{C}\ell_{n(1)}(K)$ in $Q(S)$ for A_S to be a Pólya-ring. We find that $Q(S(q, k)) = \mathscr{C}\ell_k(K)$ in the following cases:

- k is odd, cf. corollary 18;
- k is even and $T(1)$ is not cyclic, cf. corollary 18;
- $4 \mid k$ and q is odd, cf. corollary 20;
- k is even and $n(k) \neq 2n(k/2)$, cf. lemmas 21 and 19.

Thus we only have to investigate the cases where k is even and $n(k) = 2n(k/2)$. This only occurs when $q^{k/2} \in \{2, 3, 4, 5\}$, $n(1) = 2q$, k is even and $k \mid n(1) = 2q$. In all these cases there is a unique class $[c] \in \mathscr{C}\ell_0(K)$ of order 2. If $k = 2$ and q is odd we have

$$\phi_{P_0}\Big(\sum_{P \in \mathscr{C}'_q(\mathbb{F}_{q^2})} [P]\Big) = \phi_{P_0}\Big(\sum_{P \in \mathscr{C}(\mathbb{F}_{q^2})} [P]\Big) - \phi_{P_0}\Big(\sum_{P \in \mathscr{C}(\mathbb{F}_q)} [P]\Big) =$$

$$= (0, n(2)) - ([c], n(1)) = ([c], n(1)).$$

This shows that $A_{S(q,2)}$ is a Pólya-ring.

If $k = 2$ and q is even we have

$$\phi_{P_0}\Big(\sum_{P \in \mathscr{C}'_q(\mathbb{F}_{q^2})} [P]\Big) = \phi_{P_0}\Big(\sum_{P \in \mathscr{C}(\mathbb{F}_{q^2})} [P]\Big) - \phi_{P_0}\Big(\sum_{P \in \mathscr{C}(\mathbb{F}_q)} [P]\Big) =$$

$$= ([c], n(2)) - ([c], n(1)) = (0, n(1)).$$

Moreover, $([c], 0) \in \phi_{P_0}[Q(S(q, 2))]$, since $([c], 0) \in 2\mathscr{C}\ell_0(K)$, by lemma's 15 and 17. This shows that $A_{S(q,2)}$ is a Pólya-ring.

Finally, if $k \neq 2$ then $q = 2$ and $k = n(1) = 4$. We have $n(2) = 8$ and $n(4) = 16$. Under $\phi_{P_0} \circ \mathrm{Tr}_{4,1}$ the classes $[P]$, with $[P] \in \mathscr{C}'_2(\mathbb{F}_{16})$ are mapped surjectively onto $\{([a], 4), (-[a], 4)\}$, where $[a]$ is a generator of $\mathscr{C}\ell_0(K)$. In particular $(0, 4) \notin Q(S(2, 4))$, thus $A_{S(2,4)}$ is not a Pólya-ring. □

Notice that the quotient field K of $\mathbb{F}_2[X, Y]/(Y^2+XY+X^3+1)$ is a field with $q=2$ and $n(1)=4$. In fact, this is the only one, cf. [5], thm. (4.6).

5. HYPERELLIPTIC FIELDS

In this section we consider certain hyperelliptic fields. We derive results for those fields that extend the results for the elliptic case of section 3. However, we cannot be as complete in this case.

Let f be a polynomial with non-zero discriminant of odd degree in $\mathbb{F}_q[X]$, where q is a power of an *odd* prime number. We consider the hyperelliptic field K that is the quotient field of

$$\mathbb{F}_q[X, Y]/(Y^2-f).$$

Let $\mathscr{C}$ be the curve corresponding to K. Apart from an infinite point, denoted by ∞, the points of $\mathscr{C}(\mathbb{F})$ correspond to pairs $(x, y)\in\mathbb{F}^2$ with $y^2=f(x)$, for all extension fields $\mathbb{F}$ of $\mathbb{F}_q$, cf. [6] p. 26. The prime corresponding to the infinite point will be denoted by ∞ as well. Since ∞ is defined over $\mathbb{F}_q$ we have $n(k)>0$ for all $k\in\mathbb{Z}_{>0}$. Let σ be the automorphism of K defined by $\sigma X=X$ and $\sigma Y=-Y$.

We consider the case that $S=\{\infty\}$. The ring A_S is a Pólya-ring if and only if $(B(k, \infty), n(k))\in\phi_\infty[Q(\{\infty\})]=\{0\}\otimes\mathbb{Z}$ for all $k\in\mathbb{Z}_{>0}$, i.e., $B(k, \infty)=0$ for all $k\in\mathbb{Z}_{>0}$.

Let $k\in\mathbb{Z}_{>0}$ and let $P=(x_0, y_0)\in\mathscr{C}(\mathbb{F}_{q^k})$. We consider the divisor $(X-x_0)$ to find that $[P+\sigma P]=2\infty$. Thus we have

$$B(k, \infty)=\sum_{(\alpha, 0)\in\mathscr{C}(\mathbb{F}_{q^k})}([(\alpha, 0)]-\infty).$$

LEMMA 24. *Let U be a subset of the set Z of zeroes of f in $\bar{\mathbb{F}}_q$. We have $\sum_{\alpha\in U}([\alpha, 0)]-\infty)=0$ if and only if $U=\emptyset$ or $U=Z$.*

PROOF. Suppose that $\sum_{\alpha\in U}([\alpha, 0)]-\infty)=0$, then there exists a function $h(X, Y)\in K\otimes\bar{\mathbb{F}}_q$ such that h has a zero of order 1 at $(\alpha, 0)$ for all $\alpha\in U$ and h has a pole of order $\#U$ in ∞, and no other zeroes or poles. We may write $h=g_1+g_2Y$, with $g_1, g_2\in\bar{\mathbb{F}}_q[X]$. The pole at ∞ of such h has order equal to $\max\{2\deg(g_1), \deg(f)+2\deg(g_2)\}$, thus $\deg(g_1)\leq\#U/2$. We have $g_1(\alpha)=0$ for all $\alpha\in U$. We find that g_1 has more zeroes than its degree is, thus $g_1=0$. This is only possible if either $g_2=0$ and $U=\emptyset$ or $g_2\neq 0$ and $U=Z$.

THEOREM 25. *Let f be a polynomial with non-zero discriminant of odd degree in $\mathbb{F}_q[X]$, where q is a power of an odd prime number. Then $\mathbb{F}_q[X, Y]/(Y^2-f)$ is a Pólya-ring if and only if all irreducible factors of f over $\mathbb{F}_q$ have the same degree.*

PROOF. Above we have seen that the ring $\mathbb{F}_q[X, Y]/(Y^2-f)$ is a Pólya-ring if and only if $B(k, \infty)=0$ for all $k\in\mathbb{Z}_{>0}$. For fixed k we have shown that

$B(k, \infty) = 0$ if and only if either f has no zero over $\mathbb{F}_{q^k}$, or f splits completely over $\mathbb{F}_{q^k}$. This only holds for all $k \in \mathbb{Z}_{>0}$ if and only if all irreducible factors of f over $\mathbb{F}_q$ have the same degree.

6. EXAMPLES

In this chapter we present some examples, all with genus equal to 1, thus applying the results of this paper.

EXAMPLE 26. *Field of even order, ordinary case.*

We consider the quotient field K of

$$\mathbb{F}_2[X, Y]/(Y^2 + XY + X^3 + X^2 + 1),$$

which is of genus equal to 1. The corresponding curve can smoothly be embedded in 2-dimensional projective space, its points are the points $(X : Y : Z)$ with $Y^2Z + XYZ + X^3 + X^2Z + Z^3 = 0$. There are 2 points defined over $\mathbb{F}_2$, viz. $A = (0 : 1 : 1)$ *and* $B = (0 : 1 : 0)$. This shows that $\mathscr{C}\ell_0(K) \simeq \mathbb{Z}/2\mathbb{Z}$, with $[A - B]$ as its only non-trivial element. We use prop. 12(c) when $d(S) \neq 1$ and corollary 13 when $d(S) = 1$ to investigate subrings that are Pólya-rings. Using 13(b) we find that in the case that $d(S) = 1$ the ring is a Pólya-ring if and only if $[A - B] \in Q_0(S)$. The only other possibility for Pólya-rings is $d(S) = 2$. We will consider those rings where S consists entirely of primes of degree 2. There are 3 primes of degree 2, viz.

$$p_1 = \{(1 : \alpha : 1), (1 : \alpha + 1 : 1)\};$$

$$p_2 = \{(\alpha : 1 : 1), (\alpha + 1 : 1 : 1)\};$$

$$p_3 = \{(\alpha : \alpha + 1 : 1), (\alpha + 1 : \alpha : 1)\},$$

where $\alpha \in \mathbb{F}_4$ is such that $\alpha^2 = \alpha + 1$.

The divisor $(X + 1)$ equals $p_1 - 2B$, hence $[p_1] = 2[B]$.

The divisor $(Y + 1)$ equals $A + p_2 - 3B$, hence $[p_2] = [A - B] + 2[B]$.

The divisor $(Y + X + 1)$ equals $A + p_3 - 3B$, hence $[p_3] = [A - B] + 2[B]$.

If $S = \{p_1, p_2\}$, then $\phi_B[Q(S)]$ is generated by $\phi_B(p_1) = (0, 2)$ and $\phi_B(p_2) = = ([A - B], 2)$, hence A_S is a Pólya-ring. If S is equal to $\{p_1\}$ or $\{p_2, p_3\}$, then $\phi_B[Q(S)]$ is generated by $(0, 2)$ and $([A - B], 2)$ respectively. We find that A_S is not a Pólya-ring. □

EXAMPLE 27. *Field of even order, supersingular case.*

We consider the quotient field K of

$$\mathbb{F}_2[X, Y]/(Y^2 + Y + X^3),$$

which is of genus equal to 1. The corresponding curve can smoothly be embedded in 2-dimensional projective space, its points are the points $(X : Y : Z)$ with $Y^2Z + YZ^2 + X^3 = 0$. There are 3 points defined over $\mathbb{F}_2$, viz. $A = (0 : 0 : 1)$,

$B=(0:1:1)$ and $C=(0:1:0)$. This shows that $\mathscr{C}\ell_0(K)\simeq\mathbb{Z}/3\mathbb{Z}$, with $[A-C]$ and $2[A-C]=[B-C]$ as its only non-trivial elements. We use prop. 12(a) for the case that $d(S)\neq 1$ and corollary 13(a) for the case that $d(S)=1$ to investigate subrings that are Pólya-rings. Using 13(a) we find that in the case that $d(S)=1$ the ring is always a Pólya-ring. The only other possibility for Pólya-rings is $d(S)=3$. We will consider those rings where S consists entirely of primes of degree 3. There are 2 primes of degree 3, viz.

$$p_1=\{(\beta+1:\beta^2+\beta:1),(\beta^2+1:\beta:1),(\beta^2+\beta+1:\beta^2:1)\};$$

$$p_2=\{(\beta+1:\beta^2+\beta+1:1),(\beta^2+1:\beta+1:1),(\beta^2+\beta+1:\beta^2+1:1)\},$$

where $\beta\in\mathbb{F}_8$ is such that $\beta^3=\beta+1$.

The divisor (X^2+Y+X) equals $A+p_1-4C$, hence $[p_1]=2[A-C]+3[C]$.

The divisor $(X^2+Y+X+1)$ equals $B+p_2-4C$, hence $[p_2]=[A-C]+3[C]$.

If $S=\{p_1,p_2\}$, then A_S is a Pólya-ring by theorem 23. If S is equal to $\{p_1\}$ or $\{p_2\}$, then $\phi_C[Q(S)]$ does not contain $(0,3)$, thus A_S is not a Pólya-ring. □

EXAMPLE 28. *Field of odd order.*

We consider the quotient field K of

$$\mathbb{F}_3[X,Y]/(Y^2-X^3-X^2-1),$$

which is of genus 1. The corresponding curve can smoothly be embedded in 2-dimensional projective space, its points are the points $(X:Y:Z)$ with $Y^2Z-X^3-X^2Z-Z^3=0$. There are 6 points defined over $\mathbb{F}_3$, viz. $A=(0:1:1)$, $B=(0:-1:1)$, $C=(1:0:1)$, $D=(-1:1:1)$, $E=(-1:-1:1)$ and $F=(0:1:0)$. Thus $\mathscr{C}\ell_0(K)\simeq\mathbb{Z}/6\mathbb{Z}$. We investigate the group structure. The divisor $(X-1)$ is equal to $2C-2F$, hence $[C-F]$ is the unique element of order 2. The divisor $(Y+X)$ is equal to $3D-3F$ and the divisor $(Y-X)$ is equal to $3E-3F$, hence $[D-F]$ and $[E-F]$ are the classes of order 3 in $\mathscr{C}\ell_0(K)$. This means that $[A-F]$ and $[B-F]$ are the classes of order 6 in $\mathscr{C}\ell_0(K)$. The divisor $(Y+X-1)$ is equal to $A+C+E-3F$, which shows that $2[A-F]=[E-F]$, i.e.,

$$3[A-F]=[C-F],$$

$$4[A-F]=[D-F],$$

$$5[A-F]=[B-F],$$

$$6[A-F]=0.$$

We use prop. 12(b) and corollary 13(b) to investigate Pólya-rings. Notice that in the case that $d(S)=1$ we may use corollary 13(b) to find that A_S is a Pólya-ring if and only if $3[A-F]\in Q_0(S)$. We will investigate Pólya-rings with $d(S)=2$ and $d(S)=3$. Rings with $d(S)=6$ can be treated analogously. We only investigate those cases where S consists entirely of primes of degree 2 or 3 respectively.

There are 3 primes of degree 2, in K:

$$p_1 = \{(i : i+1 : 1), (-i : -i+1 : 1)\};$$

$$p_2 = \{(i : -i-1 : 1), (-i : i-1 : 1)\};$$

$$p_3 = \{(i-1 : 0 : 1), (-i-1 : 0 : 1)\},$$

with $i^2 = -1$. There are 4 primes of degree 3, in K:

$$q_1 = \{(\gamma : \gamma^2 - \gamma + 1 : 1), (\gamma + 1 : \gamma^2 + \gamma + 1 : 1), (\gamma - 1 : \gamma^2 : 1)\};$$

$$q_2 = \{(\gamma : -\gamma^2 + \gamma - 1 : 1), (\gamma + 1 : -\gamma^2 - \gamma - 1 : 1), (\gamma - 1 : -\gamma^2 : 1)\};$$

$$q_3 = \{(\gamma^2 : \gamma^2 - \gamma : 1), (\gamma^2 - \gamma + 1 : \gamma^2 + \gamma : 1), (\gamma^2 + \gamma + 1 : \gamma^2 - 1 : 1)\};$$

$$q_4 = \{(\gamma^2 : -\gamma^2 + \gamma : 1), (\gamma^2 - \gamma + 1 : -\gamma^2 - \gamma : 1), (\gamma^2 + \gamma + 1 : -\gamma^2 + 1 : 1)\},$$

with $\gamma^3 = \gamma - 1$. Considering the divisors

$$(Y - X - 1) = A + p_1 - 3F;$$

$$(Y + X + 1) = B + p_2 - 3F;$$

$$(Y) = C + p_3 - 3F;$$

$$(X^2 - Y - X + 1) = A + q_1 - 4F;$$

$$(X^2 + Y - X + 1) = B + q_2 - 4F;$$

$$(X^2 - Y) = D + q_3 - 4F;$$

$$(X^2 + Y) = E + q_4 - 4F,$$

we find that

$$\phi_F(p_1) = (5[A - F], 2);$$

$$\phi_F(p_2) = ([A - F], 2);$$

$$\phi_F(p_3) = (3[A - F], 2);$$

$$\phi_F(q_1) = (5[A - F], 3);$$

$$\phi_F(q_2) = ([A - F], 3);$$

$$\phi_F(q_3) = (2[A - F], 3);$$

$$\phi_F(q_4) = (4[A - F], 3);$$

If a prime of degree 2 is in S, we use $3\phi_F(p_1) = 3\phi_F(p_2) = 3\phi_F(p_3) = = (3[A - F], 6)$ to find that A_S is a Pólya-ring. If S contains $\{q_1, q_4\}$ or $\{q_2, q_3\}$ then A_S is a Pólya-ring, since $\phi_F(q_1 + q_4) = \phi_F(q_2 + q_3) = (3[A - F], 6)$. If, however, S consists of one prime of degree 3, or of two primes of degree 3, such that $S \neq \{q_1, q_4\}$ and $S \neq \{q_2, q_3\}$ then $(3[A - F], 6)$ is not in $\phi_F[Q(S)]$, hence A_S is not a Pólya-ring. □

REFERENCES

1. Deuring, M. – Lectures on the theory of algebraic functions of one variable, Berlin etc.: Springer Verlag, LNM **314** (1973).
2. Ireland, K., Rosen, M. – A classical introduction to modern number theory, Berlin etc.: Springer Verlag, GTM **84** (1984).
3. Joly, J.-R. – Équations et variétés algébriques sur un corps fini, L'Enseignement Math. **19**, 1 – 117 (1973).
4. Put, M., van der – private communication.
5. Schoof, R.J. – Nonsingular plane cubic curves over finite fields, to appear in J. Comb. Th.
6. Silverman, J.H. – The arithmetic of elliptic curves, Berlin etc.: Springer Verlag, GTM **106** (1986).
7. Tate, J., The arithmetic of elliptic curves, Invent. Math. **23**, 179 – 206 (1974).
8. Zantema, H. – Integer valued polynomials over a number field, Manuscripta Math. **40**, 155 – 203 (1982).